Administrator Guide: SAP Access Control 12.0

THE BEST RUN **SAP**

Content

1   Document History

Version	Date	Description
1.0.0	2018-03-28	Initial release
1.1.0	2018-07-31	Updated component diagram
		Added SAP Note for: Additional IMG documentation
		Added SAP Note for: Support pack compatibility matrix
		Added additional information about Fiori apps and configuration
1.2.0	2018-08-15	Added information for optional HANA plug-in
		Updated procedure to setup Fiori business catalogs
1.2.1	2018-08-28	Corrected typo for front-end component: UIGRC001 to UIGRAC01 100

2 Getting Started

SAP Access Control is an enterprise software application that enables organizations to control access and prevent fraud across the enterprise, while minimizing the time and cost of compliance. The application streamlines compliance processes, including access risk analysis and remediation, business role management, access request management, emergency access maintenance, and periodic compliance certifications. It delivers immediate visibility of the current risk situation with real-time data.

2.1 About This Document

The Administrator Guide for SAP Access Control 12.0 contains information on the technical system landscape, procedures and requirements for installation, and procedures and tools for the maintenance and operation of solution post-installation.

> **i Note**
>
> The access control solution is part of the SAP Governance, Risks, and Compliance suite of solutions. Some components are shared between the solutions. Therefore, this guide may contain information about shared components where relevant. In addition, for convenience, we may use the abbreviated convention **GRC** within this guide.

Integration Scenarios

The access control solution also has integration scenarios with other solutions, such as SAP Cloud Identity Access Governance, access analysis service, SAP SuccessFactor Employee Central, and others.

These integrations are done after the access control solution is installed, and in addition to the implementation procedures in this guide.

For details and information about implementing the integration scenarios, see the respective integration guides at https://help.sap.com/viewer/p/SAP_ACCESS_CONTROL.

2.2 Additional Resources

Content	Location
SAP Help Portal	http://help.sap.com
Sizing, calculation of hardware requirements such as CPU, disk, and memory resources with the *Quick Sizer* tool	https://www.sap.com/about/benchmark/sizing.quick-sizer.html#quick-sizer
Released platforms and technology related topics such as maintenance strategies and language support	https:sap.com/products To access the *Platform Availability Matrix* go to https://support.sap.com/en/release-upgrade-mainte-nance.html
Security Guides The security guides describe the settings for a medium security level and offer suggestions for raising security levels.	For the Access Control 12.0 Security Guide, go to https://help.sap.com/viewer/p/SAP_ACCESS_CONTROL. For the SAP NetWeaver Security Guide, go to https://help.sap.com/viewer/p/SAP_NETWEAVER_750. Open the relevant guide under the *Security* section.
Performance	http://help.sap.com
Information about Support Package Stacks, latest software versions, and patch level requirements	https://support.sap.com/swdc
SAP NetWeaver	https://help.sap.com/viewer/p/SAP_NETWEAVER

2.3   Important SAP Notes

You must read the following SAP Notes before you start the installation. These SAP Notes contain the most recent information on the installation as well as corrections to the installation documentation. Make sure that you have the latest version of each SAP Note, which you can find on SAP Support Portal at https://support.sap.com/.

SAP Note Number	Title
2620641	SAP Access Control 12 Release Information Note
2647067	Release Information Note for UI component for SAP Access Control 12.0.
2602131	Release strategy and Maintenance Information for the ABAP add-on **GRCFND_A V1200**

SAP Note Number	Title
2612335	Release strategy and Maintenance Information for the ABAP add-on GRCFND_A V8100
2602564	Release strategy and Maintenance Information for the ABAP add-on GRCPINW V1200_750
2602825	Release strategy and Maintenance Information for the ABAP add-on **GRCPIERP V1200_S4**
2622112	Access Control 12.0 Support Package 01 - Master Note
2641804	ESH: Accesses to search-related metadata take a long time: Symptoms may include long response time or even timing out when opening NWBC, Enterprise Portal, or Fiori Launchpad.
2672441	**AC12 IMG Additional Documentation** Documentation nodes accompany each IMG activity to explain the functionality. In rare instances where the documentation node is missing or insufficient, you can find the documentation in this SAP note.
986996	Explanation of delivered risk analysis and remediation rules.

2.4   SAP Fiori Apps

For more information about available SAP Fiori apps for access control, see *SAP Fiori 1.0 for SAP solutions for GRC* on the SAP Access Control product page: http://help.sap.com/grc-ac .

For information about installation of the SAP Fiori Launchpad, and the business catalogs and roles for access control, see chapter Setting Up SAP Fiori Launchpad Content for Front-end System [page 29].

3 Product Technical Overview

3.1 Software Components

The following table illustrates the software component matrix for the application:

Required or Optional	Component/Version	Description
Required	SAP NetWeaver 7.52 SP00	Foundation application layer on GRC system
Required	SAP Access Control 12.0 SP00	Access control application on GRC system
Optional	UIGRAC01 100	SAP Fiori UI component on frontend system
Optional	SAP Enterprise Portal 7.x	Versions 7.02 -7.31 use the 7.02 Plug-In Version 7.31 and above use the 7.31 Plug-In

The following table lists the plug-in components for target systems.

> ⓘ Note
>
> For the most updated information on plug-ins and support pack levels, see SAP note: 1352498 - *Support Pack Numbering GRC Access Control*.

Required or Optional	Component	Version	Description
Optional	GRCPINW V1200_750	SAP GRC PLUGIN NW 7.50	Access control integration with ERP non-HR functions for NW 7.50
Optional	GRCPIERP V1200_S4	SAP GRC PLUGIN S4HANA 1610+	Access control integration with S4HANA/ERP HR functions
Optional	GRCPIERP V1100_700	SAP GRC 10.1 Plug-in ERP 7.00	Access control integration with ERP HR functions

Required or Op-tional	Component	Version	Description
Optional	GRCPINW V1100_710	SAP GRC 10.1 Plug-in NW 7.10	Access control integration with ERP non-HR functions for NW 7.10
Optional	GRC 10.1 Java Components	SAP GRC AC Portal Plug-in	Portal integration for back-end systems. **i Note** There is no Portal plug-in for AC12, therefore use the GRC 10.1 plug-in.
Optional	HCO_GRC_PI	SAP GRC 10.1 Plug-in for HANA	SAP GRC 10.1 Plug-in for HANA **i Note** There is no new HANA plug-in for AC12, therefore use the GRC 10.1 plug-in.

3.2 Component Diagram

The following figure illustrates the technical landscape for the SAP Access Control solution.

Access Control 12.0 Release
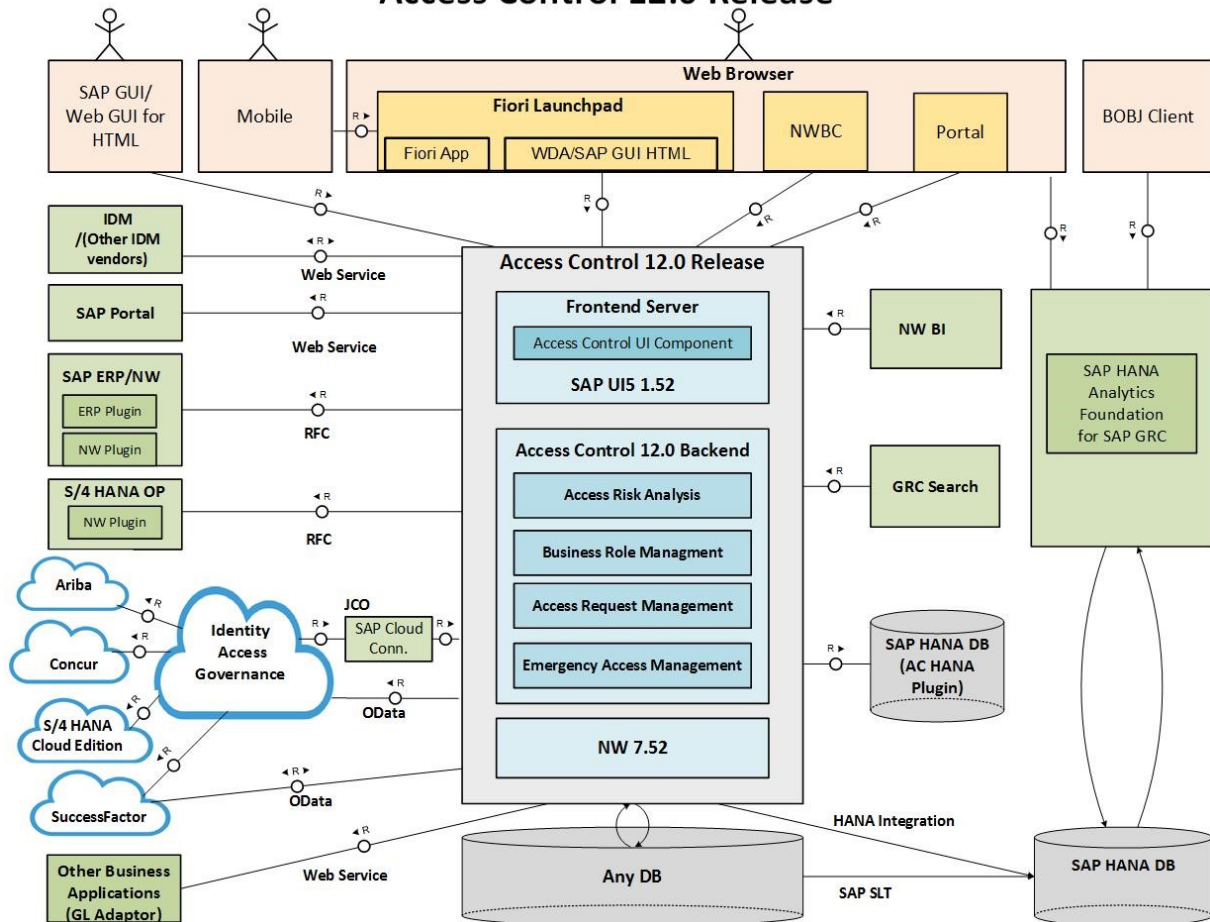
→ Recommendation

As a best practice, we recommend implementing the access control solution in three phases, with separate systems for each:

- Development
- Testing
- Production

⚠ Caution

We strongly recommend that you use a minimal system landscape for test and demonstration purposes only. For performance, high availability, and security reasons, do not use a minimal system landscape as your production landscape.

3.3 Overall Implementation Sequence

Use

This section describes the sequential implementation steps required to install the application. It includes references to the relevant installation documentation and SAP Notes.

The following table lists all the software components that you need for the installation. To implement a specific access control scenario, you may need only a subset of the software components.

The access control solution supports all the operating and database software systems that are supported by SAP NetWeaver.

> **i Note**
>
> For more information, see the product availability matrix posted https://support.sap.com/en/release-upgrade-maintenance.html .

Procedure

To install the application, use the steps described below.

Step	Required/ Optional	Action	Reference
1	Required	Install NetWeaver 7.52 SP00 on the GRC system	https://help.sap.com/viewer/p/SAP_NETWEAVER
2	Required	Install GRCFND_A V1200: Add-on Installation on the GRC system	For more information, see SAP Note: 2602131
3	Required	Install SAP Access Control 12.0 NetWeaver Plug-In (GRCPINW V1200_750) on the Plug-in system	For more information, see SAP Note: 2602564
4	Optional	Install SAP Access Control ERP Plug-In on the Plug-In system (GRCPIERP V1100_700)	For more information, see SAP Note 1855405 If SAP HR is installed, you must install GRCPIERP.
5	Optional	Install SAP GRC PLUGIN for S4HANA 1610+ (GRCPIERP V1200_S4)	For more information, see SAP Note: 2602825

Step	Required/Optional	Action	Reference
6	Optional	Install SAP Enterprise Portal 7.x	https://help.sap.com/viewer/p/SAP_NETWEAVER

4   Installation

4.1   Planning

Use

Perform the following planning steps before you start the installation.

Procedure

1. Download and check the relevant SAP Notes listed in this document.
2. Before you begin your installation, make sure that SAP NetWeaver 7.52 SP00 (ABAP) is properly installed and configured as described later in this guide. This step is *mandatory.*

   > i Note
   >
   > SAP Access Control 12.0 runs on SAP NetWeaver 7.52 SP00 HANA or non-HANA databases.

3. SAP Access Control 12.0 requires that you install plug-ins for your ERP system as directed in this guide.

   > i Note
   >
   > If you want to manage access for HANA, you must install the HANA plug-in. For more information, see the section of this guide called *Installing the SAP HANA Plug-In.*

4. Take all applicable security measures. For more information, see the *SAP Access Control 12.0 Security Guide* at http://help.sap.com/grc-ac.
5. (Optional) If you want to use the SAP NetWeaver Portal, which is not required if you use the SAP Business Client (NWBC), install the following programs:
   - GRCPIERP Portal Plug-In
   - GRC_POR_1000 (this replaces NWBC)
6. (Optional) If you plan to use Simplified Access Control, ensure that your browser is HTML5 and CSS3 compliant. Examples of such browsers include Internet Explorer 9, Chrome, and Firefox.
7. (Optional) If you want to use the SAP Fiori Launch pad, review and follow the instructions at https://help.sap.com/viewer/p/SAP_FIORI_LAUNCHPAD.
8. (Optional) If you want to use Adobe Document Services, install SAP NetWeaver Java.

> **i Note**
>
> To enable printing from SAP software, download the Adobe Document Services license. For more information, see the SAP Library at http://help.sap.com and search on *Licensing Adobe Document Services*. Also see SAP Note 736902 , *Adobe Credentials*.

4.1.1 Product Availability Matrix

https://apps.support.sap.com/sap/support/pam

SAP regularly publishes the following information about SAP software releases through the Product Availability Matrix (PAM):

- Release type (for example, standard release, early adoption release, or focused business solution release)
- Planned availability
- Maintenance durations
- Upgrade paths
- Platform availability, including database platforms and operating systems

For more information, see Product Availability Matrix for SAP Access Control 12.0 .

4.1.2 Support Pack Numbering and Compatibility

The support pack numbering of SAP Access Control support packs is dependent on the platform (Java or ABAP) as well as the Basis version of the back-end (4.6C, 620, 640 or 700+). The differences in numbering between these components makes it difficult to ascertain which support packs to apply.

It is very important that the support pack level of the front-end Java component and back-end ABAP Real-Time Agent (RTA) are in sync.

Use the information in the following SAP Note to ensure your system is appropriately patched and in synch: 1352498 Support Pack Numbering - SAP Access Control.

4.2 Preparing to Install SAP Access Control 12.0

Install the access control solution on a standalone system as opposed to installing them along with an SAP Business Suite or with any SAP Business Suite components such as ERP, SCM, CRM, OR SRM.

4.3   SAP NetWeaver Components

Depending on your landscape configuration, the following SAP NetWeaver components are available to install:

Component	Details
Support Package Manager (SPAM) 7.40 or higher	N/A
SAP Basis	7.52 SP00
SAP ABA Cross Application Component	7.52 SP00
SAP_GWFND SAP - Gateway Foundation	7.52 SP00
SAP User Interface Technology	7.52 SP00
SAP BW – SAP Business Warehouse	7.52 SP00
DMIS 2010_1_700	2011_1_731 SP10 (or latest)
(Optional) SAP NetWeaver Application Server Java for Adobe Document Services	SAP NetWeaver Java is required to use Adobe Document Services. It must be available in the system landscape, but does not need to be installed on the same system as the access control solution. You must create and activate the following JCo destinations: • WD_ALV_METADATA_DEST • WD_ALV_MODELDATA_DEST It is essential to create Adobe Credentials; see SAP Note 736902 . If problems occur in forms processing, see SAP Note: 944221 for troubleshooting.

4.4   Java Components

The Java components, SAP GRC Portal, and SAP GRC Portal Plug-Ins are supported on all SAP NetWeaver releases from 7.02 and higher. See the software compatibility matrix to determine the versions of SAP NetWeaver, SAP GRC Portal Content, and SAP GRC Portal Plug-Ins that work together.

> i Note
>
> The 10.0 version of the Java components is used with the SAP GRC 10.1 system and is also applicable for SAP Access Control 12.0.

4.5   Downloading and Installing Product Versions

You use different tools to download and install product versions.

We recommend that you use Software Provisioning Manager (in case of a new installation) or Software Update Manager (in case of a system update) in combination with the Maintenance Planner to download, install, and update product versions. This facilitates SAP NetWeaver-based application installations, system upgrades and updates (including support package stack updates), while offering a harmonized UI.

Software Provisioning Manager and Software Update Manager are shipped as part of the software logistics toolset (SL Toolset) 1.0 – independently of the applications. You can download these tools from the download center on SAP Support Portal at http://support.sap.com/swdc .

Maintenance Planner is the central point of access for all maintenance activities. It supports the installation of updates and upgrades and completely manages the maintenance activities for your whole solution. Maintenance Planner calculates the required software components, enables the download of archives, and creates a stack configuration file. You can find more information on SAP Help Portal at http://help.sap.com/viewer/p/MAINTENANCE_PLANNER.

4.5.1 Downloading SAP Access Control 12.0

1. Go to the SAP Software Distribution Center on at https://support.sap.com/swdc .
2. Download the access control solution.

   ▶ *Software Downloads* ❯ *Installations and Upgrades* ❯ *A - Z Index* ❯ *G* ❯ *SAP GRC Access Control* ❯ *SAP Access Control 12.0* ❯

4.5.2 Installing the SAP HANA Plug-In

Use

Install the following Plug-In if you are using the SAP HANA database:

Technical name	HC0_GRC_PI
Software Component Version	SAP GRC 10.1 Plug-in SAP HANA or higher

Procedure

You download this plug-in as follows:

1. Go to https://support.sap.com/swdc .
2. Choose ⏵ *Software Downloads* ❯ *Installations and Upgrades* ❯ *A - Z Index* ❯ *G* ❯ *SAP GRC Access Control* ❯ *SAP Access Control* ❯ *SAP Access Control 10.1* ❯ *Installation* ❳
3. Select the HCO_GRC_PI download object.

More Information

For more information, see SAP Note 1597627 SAP HANA Connection.

5   Post-Installation

After downloading and installing the files described in the previous sections, configure the product by following the post-installation sections in the order that they are presented.

5.1   Activating the Applications in Clients

Use

After the installation is complete and the access control solution is in place, you must activate them in each client.

Procedure

Complete the following steps to activate the applications:

1. Open the SAP Reference IMG iby going to ▐▶ *Tools* ❯ *Customizing* ❯ *IMG* ❯ *Execute Project (transaction SPRO)* ▶.
2. Display the SAP Reference IMG.
3. Choose ▐▶ *Governance, Risk, and Compliance* ❯ *General Settings* ❯ *Activate Applications in Client* ▶.
4. Execute *Activate Applications in Client*.
5. Activate an application component:by following the steps below:
   1. Choose the *New Entries* pushbutton.
   2. Select an application component from the dropdown list.
   3. In the *Active* column, select the check box for each application that you want to use.
   The application component activation is now complete.

1. Choose the *New Entries* pushbutton.
2. Select an application component from the dropdown list.
3. In the *Active* column, select the check box for each application that you want to use.

The application component activation is now complete.

5.2 Checking SAP ICF Services

Use

Specific Internet Communication Framework (ICF) SAP Services, and SAP GRC services need to be activated. They are inactive by default after an installation or an upgrade. Check that all the relevant services are active.

For more information about activating these services, see SAP Note 1088717 , *Active services for Web Dynpro ABAP in transaction SICF*.

Procedure

1. Activate each of the following ICF service nodes:
    - `/sap/public/bc`
    - `/sap/public/bc/icons`
    - `/sap/public/bc/icons_rtl`
    - `/sap/public/bc/its`
    - `/sap/public/bc/pictograms`
    - `/sap/public/bc/ur`
    - `/sap/public/bc/webdynpro`
    - `/sap/public/bc/webdynpro/mimes`
    - `/sap/public/bc/webdynpro/adobeChallenge`
    - `/sap/public/bc/webdynpro/ssr`
    - `/sap/public/bc/webicons`
    - `/sap/public/myssocntl`

    > **i Note**
    >
    > You can also activate all ICF services within:
    > - `/sap/public`
    > - `/sap/bc`
    > - `/sap/grc`

2. Activate all GRAC services.
3. Activate all services under `/sap/bc/webdynpro/sap`.

5.3   Configuring the SAP NetWeaver Gateway

Use

In order to use some of the new functionality in the access control solution, such as the *Remediation View* in SAP Access Risk Analysis, an SAP NetWeaver Gateway connection must be established. Follow these steps to maintain or verify the connector.

Procedure

1. Logon to an SAP NetWeaver system and access the SAP Reference IMG as follows: from the SAP Easy Access menu, choose ▶ *Tools* ❯ *Customizing* ❯ *IMG* ❯ *Execute Project (transaction SPRO)* ❯.
2. Choose ▶ *SAP Reference IMG* ❯ *SAP NetWeaver* ❯ *Gateway* ❯ *OData Channel* ❯ *Configuration* ❯ *Connection Settings* ❯ *SAP NetWeaver Gateway to SAP System* ❯.
3. Choose *Manage RFC Destinations* and create an RFC (communication) destination that points to the system itself.

> ⚠ Caution
>
> Be sure to specify the proper RFC Type, client, and user information using the naming convention:
>
> `<System SID>`CLNT`<Client Number>`; for example, `GD1CLNT200`.

4. If you are using Single-Signon, choose *Define Trust for SAP Business Systems*. Complete the fields with the information you provided in the Step 3.

> **i** Note
>
> This step *only* applies if you are using Single-Signon.

5. Choose *Manage SAP System Aliases* to create the system alias for the RFC destination that you created in Step 3.
6. Choose *New Entries* and enter the following values:

Field Name	What You Enter
SAP System Alias	Enter the name of the RFC destination that you created in Step 3.
Description	Enter a description that is meaningful to your installation.

Field Name	What You Enter
RFC Destination	Enter the name of the RFC destination that you created in Step 3.
Software Version	Choose the value `DEFAULT` from the drop down list.

7. *Save* your entries.
8. If required, choose *Activate or Deactivate SAP NetWeaver Gateway* to activate the SAP NetWeaver Gateway Services.
9. Choose ▎ *SAP NetWeaver* ❯ *Gateway* ❯ *OData Channel* ❯ *Administration* ❯ *General Settings* ▎.
10. Choose *Activate and Maintain Services*. The system displays a list of all the services that have been created in the backend system.
11. Click to select the *Technical Service* GRAC_GW_VIOLSUMM_REM_SRV.
12. In the *System Aliases* section (bottom right-hand corner), click *Add System Alias.*
13. Enter **GRAC_GW_VIOLSUMM_REM_SRV_0001** as the *Service Doc. Identifier*.
14. For the *SAP System Alias*, enter the system alias name that you created in Step 6.
15. Click the check box for *Default System*.
16. *Save* your entries.
17. On the *Activate and Maintain Services* screen, in the ICF Node section (bottom left-hand corner), verify that the traffic light in front of the ICF Node is green. If it is not, click the ICF Node field and select *Activate* from the ICF Node dropdown menu.
18. If required, *Save* your settings.
19. You may need to perform additional activations depending on what has already been activated in your environment. To do so, on the *Activate and Maintain Services* screen, repeat steps 11 through 18 for the following services:

Technical Service Name	External Service Name	Service Doc Identifier
/IWFND/SG_MED_CATALOG	CATALOGSERVICE	/IWFND/SG_MED_CATALOG_0001
/IWFND/SG_USER_SERVICE	USERSERVICE	/IWFND/SG_USER_SERVICE_000

> **i Note**
>
> This step is optional. It may not be required in some environments where the services have already been activated.

More Information

For more information, see the SAP Help portal at http://help.sap.com and search for: *SAP NetWeaver Gateway Developer Guide*. Then choose ▎ *OData Channel* ❯ *Basic Features* ❯ *Service Life-Cycle* ❯ *Activate and Maintain Services* ▎.

5.4 Maintaining System Data

Complete the Add-On Product Version in your system data application so that customer support can see access control solution implemented in your environment.

Procedure

1. Go to SAP Support Portal at https://support.sap.com/en/index.html 🔗 ▶ *My Support* ❯ *Systems & Installations* ❯ *System Data* ❯ *Manage Systems* ❯.
2. Use the search function provided to select an installed SAP system..
3. On the *System* tab, scroll down to the *Add-On/Enhancement Pack* section.
4. Insert a line.
5. Select the **SAP Access Control 12.0** package from the list.
6. Save your changes.
7. Repeat this procedure for all SAP systems.

5.5 Maintaining Plug-in Settings

Use

Once you install the plug-in components, Non-HR (GRCPINW), and, optionally, HR (GRCPIERP), you must maintain the plug-in user exit and configuration settings.

Procedure

In the IMG activity below, you maintain the user exit settings that are required to run Risk Terminator in Role Maintenance (transaction PFCG). Risk Terminator enables real time risk analysis while making changes to role authorizations or role assignments in the Plug-In system.

1. Open the SAP Reference IMG from ▶ *Tools* ❯ *Customizing* ❯ *IMG* ❯ *Execute Project (transaction SPRO)* ❯.
2. Display the SAP Reference IMG.
3. Open ▶ *Governance, Risk, and Compliance (Plug-In)* ❯ *Access Control* ❯.
4. Maintain the necessary IMG activities for your system according to the instructions in the IMG documentation that is located at the left of each of the following IMG nodes:
   ○ *Maintain User Exits for Plug-in Systems*

     o   *Maintain Plug-in Configuration Settings*

5.6   Activating Crystal Reports

To use the Crystal Reports function, activate the flag *Allow Crystal Reports* in Customizing under ▐▶ *SAP NetWeaver* ❯ *Application Server* ❯ *SAP List Viewer (ALV)* ❯ *Maintain Web Dynpro ABAP-Specific Settings* ▐.

5.7   Activating BC Sets

BC sets are delivered implementation toolsets that simplify the Customizing process. You activate Business Configuration (BC) sets after the software is installed.

> ⚠ Caution
>
> You can activate a BC set *only* if that client is *not a production client*. When you activate the BC set, all data in the BC set is transferred into the corresponding tables and any existing entries are overwritten.

> → Recommendation
>
> Always consult with the functional experts for your application before activating any of the BC sets.

See *SAP Solution Manager* for information about Customizing activities at https://support.sap.com/solutionmanager .

For more information about BC sets, see https://help.sap.com/viewer/p/SAP_NETWEAVER_750.

Procedure

1. From the SAP Easy Access screen, choose ▐▶ *Tools* ❯ *Customizing* ❯ *IMG* ❯ *Execute Project* ❯ *SAP Reference IMG* ▐.
2. Choose *Existing BC Sets* from the toolbar in the *Implementation Guide* to identify all of the IMG activities that have BC sets.
3. Select one of these IMG activities and choose the *BC Sets for Activity* button.
   The system displays the contents of the BC set in a new window.
4. To activate this BC set, choose the pull-down menu ▐▶ *Go to* ❯ *Activation Transaction* ▐.
5. Select the icon for *Activate BC Set* (or use **F7**).
   The *Activation Options* screen opens.
6. Choose *Continue*.
   A completion message appears: *Activation successfully completed*. If a yellow informational message appears, choose *Enter* and then the completion message appears.

> **i Note**
>
> A message with a **yellow** background is only a warning and you can proceed. A message with a **red** background is an error message and you must resolve the error. If you receive a Basis error message with a red background, contact your system administrator.

5.7.1 SAP Access Control BC Sets

The following tables list the BC sets for the access control solution categorized by type. BC sets marked with an asterisk (*) indicate that you can also activate them in Customizing.

> **→ Recommendation**
>
> Always consult with the access control solution functional experts before activating the BC sets for rules such as *Segregation of Duties (SoD)*to determine which rule sets are relevant for your implementation.

BC Set	BC Set Name
Specific to Access Risk Analysis	
`GRAC_RA_RULESET_COMMON`	SoD Rules Set
`GRAC_RA_RULESET_JDE`	JDE Rules Set
`GRAC_RA_RULESET_ORACLE`	ORACLE Rules Set
`GRAC_RA_RULESET_PSOFT`	PSOFT Rules Set
`GRAC_RA_RULESET_SAP_APO`	JDE Rules Set
`GRAC_RA_RULESET_SAP_BASIS`	SAP BASIS Rules Set
`GRAC_RA_RULESET_SAP_CRM`	SAP CRM Rules Set
`GRAC_RA_RULESET_SAP_ECCS`	SAP ECCS Rules Set
`GRAC_RA_RULESET_SAP_HR`	SAP HR Rules Set
`GRAC_RA_RULESET_SAP_NHR`	SAP R/3 less HR Basis Rules Set
`GRAC_RA_RULESET_SAP_R3`	SAP R/3 AC Rules Set
`GRAC_RA_RULESET_SAP_SRM`	SAP SRM Rules Set
`GRAC_RA_RULESET_S4HANA_ALL`	Rule set for risk analysis integration with Fiori Apps on S/4HANA on-premise systems.
Specific to Access Request Management	

BC Set	BC Set Name
GRAC_ACCESS_REQUEST_REQ_TYPE*	Request Type
GRAC_ACCESS_REQUEST_EUP*	EUP (Note: Only the value **EU ID 999** is valid for this BC set.)
GRAC_ACCESS_REQUEST_APPL_MAPPING*	Mapping BRF Function IDs and AC Applications
GRAC_ACCESS_REQUEST_PRIORITY*	Request Priority
GRAC_DT_REQUEST_DISPLAY_SECTIONS	Simplified Access Request Display Sections
GRAC_DT_REQUEST_FIELD_LABELS	Simplified Access Request Field Labels
GRAC_DT_REQUEST_PAGE_SETTINGS	Simplified Access Request Page Settings
Specific to Business Role Management	
GRAC_ROLE_MGMT_SENTIVITY*	Sensitivity
GRAC_ROLE_MGMT_METHODOLOGY*	Methodology Process and Steps
GRAC_ROLE_MGMT_ROLE_STATUS*	Role Status
GRAC_ROLE_MGMT_PRE_REQ_TYPE*	Prerequisite Types
GRAC_ROLE_SEARCH_COFIGURATION	Role Search Configuration for Access Request
Specific to Superuser Management	
GRAC_SPM_CRITICALITY_LEVEL*	Criticality Levels
Specific to Workflow	
GRC_MSMP_CONFIGURATION*	MSMP Workflow Configuration Rules Set

5.8 Run Role Name Conversion Program

Customers may use varied standards when naming roles in their landscape. This may result in failed role searches when submitting access requests. The below program is used to convert roles into upper case to improve search.

Run the GRAC_ROLE_NAME_SH_CONVERSION program to improve search capabilities and resolve potential issues from role name mismatch.

5.9   SAP Enterprise Portal Configuration

5.9.1 Creating a System Connection with the SAP Enterprise Portal

For information about how to create an SAP Enterprise Portal system connection for access control solution, see: https://help.sap.com/viewer/p/SAP_NETWEAVER_750 > SAP Enterprise Portal.

SAP provides a set of sample roles that include the recommended authorizations. You can create your own PFCG roles or copy the sample roles to your customer namespace and then modify them as needed.

For more information about the delivered roles, see the Security Guide for SAP Access Control 12.0 at https://help.sap.com/viewer/p/SAP_ACCESS_CONTROL.

5.9.2 Portal Configuration for SAP Access Control Users

The list below contains the system and portal aliases roles that you configure if you only have SAP Access Control in your system landscape.

- **System Aliases**:
    - The system alias must use `SAP-GRC`, `SAP-GRC-AC`, and SAP_GRC.
- **Portal Roles**:
    - Assign the role `GRC ACCESS CONTROL` to users.
    - Assign the role `ERP COMMON` to everyone in the user group.

> **i** Note
>
> For SAP Access Control only environments, you must assign the `GRC Access Control` role to at least one user.

5.9.3 Portal Configuration for SAP Solutions for GRC-Licensed Users

The access control solution is part of a GRC suite. If your system landscape contains more than one GRC component (SAP Access Control, SAP Process Control, or SAP Risk Management), you configure the system aliases and portal roles as follows:

System Aliases

GRC Component	System Alias Configuration
If SAP Access Control is activated:	The system alias must use `SAP-GRC`, `SAP-GRC-AC`, and `SAP_GRC`.
If SAP Process Control is activated:	The system alias must use `SAP-GRC` and `SAP-GRC-PC`, and `SAP_GRC`
If SAP Risk Management is activated:	The system alias must use `SAP-GRC` and `SAP-GRC-RM`, and `SAP_GRC`.

Portal Roles

Assign to	Role Name
User	`GRC SUITE`
Everyone in the user group	`ERP COMMON`
User, if needed	`GRC Internal Audit Management`

5.9.4 Creating the Initial User in the ABAP System

The access control solution uses various roles to interface with the SAP system. This section explains how to create your initial ABAP system user for SAP Access Control.

> **i Note**
>
> This section uses the delivered roles as examples only. As you complete the procedure, you must replace the delivered roles with equivalent roles in your customer namespace.

Procedure

1. Assign all access control users the role `SAP_GRAC_BASE` so they can access the access control applications.
2. Assign the role `SAP_GRAC_ALL` to the user who will perform Customizing. This role is the power user role. It gives the designated user the ability to see and do everything without being assigned to a specific SAP

Access Control role. This role is typically assigned to the user who creates the organization structures and assigns the business roles to all the other users.

> **i Note**
>
> The role does not contain the authorizations for Workflow Customizing, Case Management, or web services activation. For these authorizations, use the role `SAP_GRAC_SETUP`.

> **⚠ Caution**
>
> Assign the `SAP_GRAC_ALL` role carefully, since a user assigned to this role can make pervasive changes.
>
> For more information on the `SAP_GRAC_ALL` role and its authorizations, see the Security Guide at: https://help.sap.com/viewer/p/SAP_ACCESS_CONTROL .

3. Using transaction `SU01`, create a user.
4. If this user needs to receive workflow notifications via e-mail, on the *Address* data tab, assign an e-mail address and a *Comm. Meth* of *E-Mail* to the user.
5. On the *Roles* tab, assign the roles `SAP_GRAC_BASE` and `SAP_GRAC_ALL` to this user.
6. This user can now use transaction `SPRO` to complete the Customizing configuration including such steps as activating the Business Configuration (BC) sets and assigning roles to other users
.

5.9.5 Creating the Initial User in the SAP Enterprise Portal

The navigation tabs and work centers for SAP Access Control are defined in the portal roles that are maintained in the SAP GRC portal package.

After creating the portal user, the portal administrator must assign to that user the SAP GRC portal roles. These portal roles enable the user to see the SAP GRC navigation and work centers tabs.

> **i Note**
>
> This section uses the delivered roles as examples As you complete the procedure, you must replace the delivered roles with equivalent roles in your customer namespace.

Procedure

1. Log on as the portal user administrator and access the *User Administration* function.
2. If a user has already been created by the `User Management Engine(UME)` that is connected to the SAP GRC ABAP system, you do not need to create a user in the portal system.
   If a user has not been created by the `User Management Engine(UME)`, create a new portal user and assign the SAP GRC ABAP system to the user in the *User Mapping for System Access* tab, along with a mapped user ID and password.
3. Go to the *Assigned Roles* tab and assign the role *GRC Suite* (name: `pcd:portal_content/ com.sap.pct/com.sap.grc.grac/com.sap.grc.ac.roles/com.sap.grc.ac.Role_All`) to the

user who has the power user role `SAP_GRAC_ALL` in the ABAP system. This role enables the power user to view the work centers.

More Information

For more information about the visibility of work centers, see the Security Guide at: https://help.sap.com/viewer/p/SAP_ACCESS_CONTROL .

This information is based on the technologies delivered by SAP NetWeaver Portal. For more information, see the *Portal Security Guide* athttp://help.sap.com/saphelp_spm21_bw/helpdata/en/5c/429f00a14aa54195b1c63ae1512d10/frameset.htm .

5.10 Setting Up SAP Fiori Launchpad Content for Front-end System

The SAP Fiori Launchpad is a shell that hosts SAP Fiori apps, and provides the apps with services such as navigation, personalization, embedded support, and application configuration. SAP Access Control 12.0 SP00 delivers a set of SAP Fiori business catalogs that enable you to open the Web Dynpro Access Control applications in the launchpad.

This section describes the procedure to add the access control business catalogs to your launchpad. The procedure is relevant only for landscapes using SAP Fiori Launchpad.

The access control back-end component contains the technical catalog containing information about the tiles, which we call the app descriptors. The front-end component `UIGRAC01 100` contains the business catalogs and business roles. We replicate the technical catalog from the back end into the front end to establish a connection between the technical catalog and the business catalog.

Prerequisite

You have installed the front-end component `UIGRAC01 100`. The component contains the contains the business catalogs and business roles for SAP Access Control 12.0.

There are three main steps to configuring the business catalogs for access control:

1. Create RFC Connections
2. Map the RFC Connections
3. Replicate the Technical Catalog from the Back-end System

These steps are described in more detail in the sections below.

For additional information, see Implementation Tasks on the Front-end Server in the UI Technology Guide for S/4HANA.

Create RFC Connections

1. In the front-end system start transaction `SM59`.
2. Create two RFC connections: one of type `ABAP Connection` and one of type `H – HTTP connection to ABAP System`
   Use the following naming conventions:
   - **ABAP connection: <Logical System Alias>_RFC**
   - **HTTP connection: <Logical System Alias>_HTTP or <Logical System Alias>_HTTPS**

   > → Recommendation
   >
   > We recommend using an HTTPS connection. Set the SSL option to *Active*.

   For the ABAP connection, set *Trusted Relationship* set to **Yes**, and set the *Current User* to **True**.
   For each connection, enter the *Target Host* under *Technical Settings*, and configure the settings under *Logon & Security*.

Map the RFC Connections

1. Open the maintenance view `/UI2/V_ALIASMAP`.
2. Map the connections in table: `/UI2/SYSALIASMAP` .
   Map the connections as follows:

Client	Source System Alias	Target System Alias
<Your Front-end Client>	SOHGRAC	<Logical System Alias>

Replicate the Technical Catalog from the Back-end System

1. Launch the report `/UI2/GET_APP_DESCR_REMOTE_DEV`.
2. 2. Enter the following values:
   Replication System Alias: **SOHGRAC**
   Back-end Technical Catalog ID: **SAP_TC_GRC_AC_BE_APPS**
3. Select the *Test Mode*, and choose *Execute* to test the configuration. The catalogs are not be replicated in test mode. A log is displayed showing the results.
4. If the log does not contain any errors, deselect *Test Mode* and choose *Execute* to replicate the business catalogs.

   > → Recommendation
   >
   > We recommend scheduling the report to run daily. As the report needs to run after every system update, scheduling the report to run daily ensures that you have up-to-date information in the SAP Fiori launchpad designer.

5.10.1 Business Catalogs and Roles for the Fiori Launchpad

The following business catalogs and business roles are delivered as part of the front-end component `UIGRAC01 100`.

Delivered Business Catalog Roles

Depending on your business requirement you can assign the following delivered roles to your users:

> **i Note**
>
> These roles are examples. You can copy them to your own namespace or create your own.

Delivered Business Catalog Role	Description
SAP_GRAC_BCR_CMPLNCMGR_T	Compliance Manager
SAP_GRAC_BCR_EMPLOYEE_T	Access Control Employee
SAP_GRAC_BCR_MANAGER_T	Request Approver
SAP_GRAC_BCR_REQADMINTR_T	Access Control Administrator
SAP_GRAC_BCR_SCRTYMGR_T	Security Manager

Delivered Business Catalogs

These are the corresponding delivered business catalogs.

Delivered Business Catalog Role	Description
SAP_GRAC_BCR_CMPLNCMGR_T	Compliance Manager
SAP_GRAC_BCR_EMPLOYEE_T	Access Control Employee
SAP_GRAC_BCR_MANAGER_T	Request Approver
SAP_GRAC_BCR_REQADMINTR_T	Access Control Administrator
SAP_GRAC_BCR_SCRTYMGR_T	Security Manager

5.11 Implement SAP Note: 2641804

After installation or upgrade you may need to refresh the CDS configuration.

Symptoms may include Fiori Launchpad or applications via NWBC taking a long time to open or the session timing out.

To resolve the issue, implement SAP Note 2641804 .

6   Operations

6.1   Monitoring of the Application

To monitor the access control solution, you can use Computing Center Management System (CCMS). The CCMS provides a range of monitors for monitoring the SAP environments and its components. These monitors are indispensable for understanding and evaluating the behavior of the SAP processing environment. In the case of poor performance values, the monitors provide you with the information required to fine tune your SAP system and therefore to ensure that your SAP installation is running efficiently. The transaction code is RZ20.

For information on setting up and using CCMS, see the following:

https://help.sap.com/viewer/p/SAP_NETWEAVER_750

Solution Life Cycle Management

Monitoring in the CCMS

6.1.1 Monitor Templates

You use monitor templates to specify files and search patterns to be checked for the access control solution in your system landscape.

Monitor Templates

Monitor Type	Name
CCMS Monitor Templates	Background Processing
	Performance Overview
	Syslog
SAP Web Service Monitor Template	Web Service Monitor

6.1.2 Alert Monitoring with CCMS

Proactive, automated monitoring is the basis for ensuring reliable operations for your SAP system environment. SAP provides you with the infrastructure needed to set up your alert monitoring to recognize situations for the access control solution.

> → Recommendation
>
> To enable the auto-alert mechanism of CCMS, see SAP Note 617547 .

6.1.2.1   Component Specific Monitoring

You use CCMS to monitor the following data for the access control solution:

- Background job
- Performance Overview
- DB access time
- System log
- System errors
- Web Services Call

Background Jobs

Monitor the background job status for jobs that are aborted, canceled, or have been running for a long time.

You can check the details of canceled jobs by selecting a job and clicking *Step*.

> i Note
>
> The *Program name/command* for the access control solution start with GRAC.

Performance Overview

In the *Performance Overview* templates, look for processes with a high *Response Time*. The access control solution processes begin with **GRAC**.

System Logs

Monitor system logs for any errors, such as *System Log (Syslog): Local Analysis* and *R3Syslog*. The R3Syslog displays runtime errors.

You can review the transaction codes for the access control solution for errors. You can get the complete list of access control transaction codes with transaction code SE93. Search for GRAC*.

Some of the most used codes include:

Access Control Transaction Codes

Transaction Code	Description
NWBC	Access the majority of the Access Control capabilities and reports (role: SAP_GRC_NWBC)
GRAC_ALERT_GENERATE	Alert generation
GRAC_BATCH_RA	Risk Analysis in Batch Mode
GRAC_EAM	Emergency Access Management (EAM) Launchpad Logon
GRAC_SPM_CLEANUP	Cleanup EAM (SPM) Application Data
GRACRABATCH_MONITOR	Batch Risk Analysis Monitor

System Errors

You review the *CCMS Monitor Templates (System Errors)* for error messages, such as *Aborted Batch Jobs* and *Update Errors:*.

Web Services

Monitor the *SAP Web Service Monitor Templates* for web service errors, such as:

- Task Watcher
- Supervisor Destination
- Web Services Reliable Messaging (WSRM) Event Handler
- Web Services (WS) Namespace for Inbound Destinations
- WS Service Destinations

6.1.3 Detailed Monitoring and Tools for Problem and Performance Analysis

The access control is based on SAP NetWeaver Web Application Server 7.52, and uses the tools included with SAP NetWeaver for analysis of items such as database, operating system, and workload.

In this section, we list the specific *application log* subobjects used by the access control solution.

To view **Job Logs**, use transaction SM37.

To view **Work item Logs**, use transaction SWI1.

For information about technical problem analysis within an SAP NetWeave landscape, see Technical Operations Manual for SAP NetWeaver.

6.1.3.1   Trace and Log Files

You use SAP NetWeaver transactions, such as ST22 and SM2, to monitor trace and log files. The archiving object for Access Control is GRAC_REQ.

Application Logs

The access control solution uses the SAP NetWeaver application logs to store application errors, warnings, and success messages issued in critical processes. For example, UI transactions messages are stored in the SAP NetWeaver application log. The application logs can be monitored with transaction SLG1.

The following tables list the log subobjects. The Access Control log object is GRAC.

Access Control Log Subobjects

Log Object	Log Subobjects	Description
GRAC	AUTH	Authorization check
GRAC	BATCH	Batch risk analysis
GRAC	HRTRIGGER	HR trigger
GRAC	SOD_RISK_ANALYSIS	Segregation of Duties (SOD) Risk Analysis
GRAC	SPM	Emergency Access Management log
GRAC	UAR	User Access Review (UAR)

The following table lists the GRC shared log subobjects. The shared components log object is GRFN.

GRC Foundation (shared) Log Subobjects

Log Object	Log Subobjects	Description
GRFN	AC_PROV	Access Control Provisioning Engine
GRFN	AC_REP	Access Control Repository
GRFN	API	GRC API logging
GRFN	ASYNC_UPDATE	Asynchronous Update Infrastructure
GRFN	AUTH	GRC authorization
GRFN	CASE_INT	Continuous monitoring case integration
GRFN	FDS	Continuous monitoring flexible data store
GRFN	HRMAINT	Access to HR ORG maintenance
GRFN	IO_EXPORT	IO Export
GRFN	IO_IMPORT	IO Import
GRFN	IO_META	IO Metadata
GRFN	JOB	AMF Job Step Execution
GRFN	JOB_DESIGN	AMF Job Step Design Time
GRFN	MDCHECK	Master Data Consistency Check
GRFN	MIGRATION	GRC migration
GRFN	MSMP_WF_CN	Multi-Stage Multi-Path (MSMP) Workflow – Configuration
GRFN	MSMP_WF_NT	Multi-Stage Multi-Path (MSMP) Workflow – Notification
GRFN	MSMP_WF_RT	Multi-Stage Multi-Path (MSMP) Workflow – Runtime
GRFN	OWP	Offline Workflow Process
GRFN	POLICY	Policy Management
GRFN	REPLACEMENT	GRC replacement
GRFN	REP_ENGINE	Reporting engine
GRFN	RISK_AGGR	Risk Aggregation

Log Object	Log Subobjects	Description
GRFN	RM_BANKING	Operational Risk Management for Banking Industry
GRFN	SURVEY	Survey planning

For more information about application logs, see https://help.sap.com/viewer/p/SAP_NETWEAVER_750 ▶ *Solution Life Cycle Management* ▶ *Application Log* ▶.

Job Logs

You can view job logs using transaction SM37.

Workflow Item Logs

You can view the workflow item logs using transaction SWI1.

For more information on workflows, see SAP Workflow Administration at http://help.sap.com ✎.

6.1.4 Important Application Objects

We recommend you monitor the following access control solution objects:

Objects to Monitor

Object	Tools	Description
Process Overview	Transaction SM50	The monitor tracks the amount of time critical processes such as dialog (DIA), update (UPD), or background (BGD) have been running. Processes that have been running too long are shown in red in the *runtime* column.
		Ensure there are enough background work processes on the GRC system. You can use operation mode to switch work processes.

Object	Tools	Description
Background Process	Transaction `SM37`	Select the jobs by job name, user name, status, and time period to display a status overview of scheduled jobs. Look for any canceled jobs.
Application Logs	Transaction `SLG1`	Enable the application logs for potential risk areas. For more information, see *Trace and Log Files*.
CCMS	Transaction `RZ20`	Monitor the following: • SAP buffer configuration • Database workload • Operating system workload • System logs for errors • System errors for application dumps • Workload analysis for any performance issues
Shared Objects Memory	Transaction `SHMM`	Transaction `SHMM` provides an overview of the area instances in the shared objects memory of the current application server.
Workflow event queue	`SWEQADM`	Use the event queue to delay the starting of receivers reacting to a triggering event. This spreads the system load over a longer time period to combat the threat of system overload. The system administrator sets the event queue.
`SICF`	Transaction `SICF`	Use this transaction to activate Internet services, Web services, and Web Dynpro.
`SIGS`	Transaction `SIGS`	Use this transaction to view the status of IGS services and the required parameters.

6.2   Managing the Application

SAP provides you with an infrastructure to help your technical support consultants and system administrators manage all SAP components and complete tasks related to administration and operation.

6.2.1 Starting and Stopping

The access control solution is provided as add-on components for SAP NetWeaver. You start and stop them with SAP NetWeaver Web Application Server.

> → Recommendation
>
> For more information about `STARTSAP`/`STOPSAP` and `SAPMMC`, see the Technical Operations Manual for SAP NetWeaver

6.2.2 Backup and Restore

You need to back up your system landscape regularly to ensure that you can restore and recover it in case of failure. All application data for the applications reside in the underlying database.

The applications rely on the SAP NetWeaver ABAP standard capabilities for the technical operations. The configuration data is stored in the Implementation Guide (IMG) database tables. These settings are established during the Customizing activities during implementation (transaction `SPRO`).

> i Note
>
> If you use a document management system (DMS) that stores data outside of the underlying database, refer to the backup and restore recommendations for that DMS.

6.2.3 System Copy

The access control solution uses the standard tools and procedures of SAP NetWeaver.

> i Note
>
> A client copy from one system into another system with a different operating system or database is not an alternative to a complete heterogeneous migration. For example, client copies do not ensure that all repository changes are taken over into the new system. Therefore, if you want to change your database or application server platform, a heterogeneous system copy is the only procedure that ensures full data replication.

For more information, see SAP OS/DB Migration Check at https://support.sap.com/osdbmigration ☞

6.2.4 Periodic Tasks

In addition to the standard jobs mentioned in the *Technical Operations Manual for SAP NetWeaver*, access control specific jobs must be scheduled in your system. Run all jobs, unless otherwise specified, at times of minimal system activity (so as not to affect performance or otherwise disrupt your daily operations). All jobs can be restarted. There are no dependencies between the jobs.

6.2.4.1   Scheduled Periodic Tasks

This information describes the tasks required to keep the application running smoothly. You can configure the tasks to automatically run. It is important that you monitor the execution of these tasks on a regular basis. The tasks are scheduled using transaction SM36, except for the *Background Job for Missed Deadlines*, which uses transaction SWU3.

Scheduled Periodic Tasks

Program Name/Task	Recommended Frequency	Description
Schedule Background Job for Missed Deadlines	Every 3 minutes	Specify a time interval at which the background job is called regularly. With each execution, the background job checks whether new deadlines have been missed since the last time it ran.
Schedule Job for Sending E-Mail	Every 3 minutes	This program checks whether there are new work items for Process Control and Risk Management, and determines the e-mail addresses of the work item recipients.
GRFN_AM_JOBSTEP_MONITOR	Hourly	The monitoring program to update job / job step status.
Transfer Work Items to Replacement	Daily	The program transfers work items from users that are no longer working in Process Control and Risk Management to the replacement users entered in the system for these users.
Maintain DataMart	Daily	Schedule the report GRFN_DATAMART_MAINTAIN. This can be used for maintaining and uploading the data to DataMart.

6.2.4.2 Synchronization Tasks

The following tasks are accomplished through the Customizing activities (transaction `SPRO`) found at ▶ *SAP Reference IMG* ❯ *Governance, Risk, and Compliance* ❯ *Access Control* ❯ *Synchronization Jobs* ❯.

Refer to the documentation next to each activity for detailed directions.

> **i** Note
>
> The frequencies are recommendations. Adjust them according to your business need. For example, when you are first implementing the product, you might want to run these tasks more often.

Synchronization Tasks

Customizing Task Name	Recommended Frequency	Transaction
Authorization Synch	Weekly	`GRAC_AUTH_SYNC`
Repository Object Synch (includes Profile, Role and User Synchronization)	Daily	`GRAC_REP_OBJ_SYNC`
Action Usage Synch	Daily	`GRAC_ACT_USAGE_SYNC`
Role Usage Synch	Daily	`GRAC_ROLE_USAGE_SYNC`
Firefighter Log Synch	Daily	`GRAC_SPM_LOG_SYNC`
Firefighter Workflow Synch	Daily	`GRAC_SPM_WF_SYNC`
Fetch IDM Schema	as needed	`GRAC_IDM_SCHEMA_SYNC`
EAM Master Data Synch	as needed	`GRAC_SPM_SYNC`

6.2.5 User Management

The access control solution uses SAP NetWeaver for user management.

For more information, on user roles and authorizations, see the Security Guide at https://help.sap.com/viewer/p/SAP_ACCESS_CONTROL

6.3 Data Archiving and Management

The access control solution uses the SAP Information Lifecycle Management (ILM) framework to maintain data protection and archiving.

For information on using ILM, and on the access control data and archiving objects, see the *Security Guide for SAP Access Control 12.0.*

6.4 High Availability and Load Balancing

The access control solution uses the SAP NetWeaver framework and tools for high availability and load balancing.

For more information, see the Technical Operations Manual for SAP NetWeaver

6.5 Software Change Management

Software Change Management standardizes and automates software distribution, maintenance, and testing procedures for software landscapes and multiple software development platforms. These functions support your project teams, development teams, and application support teams.

Software Change Management establishes solution-wide change management that allows for specific maintenance procedures, global rollouts (including localizations), and open integration with third-party products.

This section provides additional information about the most important software components.

The following topics are covered:

- Transport and Change Management:
  Enables and secures the distribution of software changes from the development environment to the quality assurance and production environment.
- Development Request and Development Release Management:
  Enables customer-specific maintenance procedures and open integration with third-party products.
- Template Management:
  Enables and secures the rollout of global templates, including localizations.
- Quality Management and Test Management:
  Reduce the time, cost, and risk associated with software changes.
- Support Packages and SAP Notes Implementation:
  Provide standardized software distribution and maintenance procedures.
- Release and Upgrade Management:
  Reduces the time, cost, and risk associated with upgrades.

6.5.1 Transport and Change Management

For transport and change management issues, the procedures of SAP NetWeaver apply.

> → Recommendation

For more information, see Technical Operations Manual for SAP NetWeaver.

6.5.2 Development Requests and Development Release Management

The standard procedures of SAP NetWeaver apply.

For more information, see Technical Operations Manual for SAP NetWeaver.

6.5.3 Support Packages and Patch Implementation

We recommend you implement Support Package Stacks (SP-STACKS), which are sets of Support Packages and patches for the respective product version that must be used in the given combination.

Read the corresponding Release and Information Notes (RIN) before you apply any Support Packages or Patches of the selected SP-Stack.

The RIN and support packages are available at the SAP Support Portal: http://support.sap.com/patches.

6.6 Troubleshooting

The access control solution is an add-on component for SAP NetWeaver and uses the same troubleshooting tools for the SAP NetWeaver Application server.

For more information, go to the SAP Support Portal **> Tools** at http://support.sap.com.

> **i** Note
>
> When reporting any issues for troubleshooting, use component **GRC-SAC**.

6.6.1 Configuring Remote Connection to SAP Support

SAP offers access to remote support and remote services. You have to set up a remote network connection to SAP.

For information on how to setup and use *Remote Connections*, go to https://support.sap.com/remoteconnections .

Read-Only Role

For remote support from SAP, a support user must have read-only access to the support tools. Since these applications are built upon the NetWeaver ABAP stack, a support user can use the SAP standard CSS remote support tool which is accessible through the SAPGUI or web browser.

The access control solution uses this read-only role: **SAP_GRAC_DISPLAY_ALL**.

6.6.2 Support Components

You can use the following components information when requesting support for the access control solution.

Component	Description
GRC-SAC-ARA	Access Risk Management
GRC-SAC-ARQ	Access Request
GRC-SAC-BRM	Business Role Management
GRC-SAC-EAM	Emergency Access Management

6.7 Categories of System Components for Backup and Restore

Categories of System Components	Category Properties	Suggested Methods for Backup and Restore	Examples
I	Only software, no configuration, or application data	No backup, new installation in case of a recovery	BDOC modeler
		Initial software backup after installation and upgrade	

Categories of System Components	Category Properties	Suggested Methods for Backup and Restore	Examples
		Backup of log files	
II	Only software and configuration information, no application data	Backup after changes have been applied	SAP Gateway
		No backup, new installation, and configuration in case of a recovery	Communication Station
		Backup of log files	SAP Business Connector, SAP IPC (2.0C)
III	Only replicated application data, replication time is sufficiently small for a recovery	Data	SAP IMS/Search
		No data backup needed	Engine
		Backup of software, configuration, log files	SAP IPC (2.0B)
IV	Only replicated application data, backup recommended because replication time is too long, data not managed by a DBMS	Data	SAP IMS/Search
		Application specific file system backup or	Engine
		Multiple instances	Web server
		Backup of software, configuration, log files	SAP IPC (2.0B)
V	Only replicated application data, backup recommended because replication time is too long, data managed by a DBMS	Data	SAP IPC (2.0B)
		Database and log backup or	Catalog Server
		Multiple instances	Web server
		Backup of software, configuration, log files	SAP IPC (2.0B)

Categories of Systems Components	Category Properties	Suggested Methods for Backup and Restore	Examples
VI	Original application data, standalone system, data not managed by a DBMS	Data	Web Server
		Application specific file system backup	
		Backup of software, configuration and log files	

Categories of Systems Components	Category Properties	Suggested Methods for Backup and Restore	Examples
VII	Original application data, standalone system, data managed by a DBMS, not based on SAP NetWeaver Application Server	Data Database and log backup Backup of software, configuration and log files	none available
VIII	Original application data, standalone system, based on SAP NetWeaver Application Server	Data Database and log backup, application log backup (such as job logs in file system) Backup of software, configuration and log files	Standalone SAP SAP ERP none available
IX	Original application data, data exchange with other systems, data not managed by a DBMS	Data Application specific file system backup, data consistency with other systems must be considered Backup of software, configuration, log files	none available
X	Original application data, data exchange with other systems, data managed by a DBMS, not based on SAP NetWeaver Application Server	Data Database and log backup, data consistency with other systems must be considered Backup of software, configuration, log files	SAP Live Cache SAP Mobile Workbench
XI	Original application data, data exchange with other systems, based on SAP NetWeaver Application Server	Data Database and log backup, application log backup (such as job logs in the system), data consistency with other systems must be considered Backup of software, configuration, log files	SAP ERP SAP CRM SAP APO SAP NetWeaver Business Warehouse

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon   : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:

    - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
    - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.

- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

THE BEST RUN SAP